ORACLE DATA MASKING PACK

THE INDUSTRY'S HIGH PERFORMANCE MASKING SOLUTION FOR ORACLE DATABASE APPLICATIONS

Organizations can inadvertently breach data privacy rules when they copy sensitive or regulated production data into non-production environments. These data breaches incur significant costs to the organizations that have to remediate the problem immediately and deal with the harm caused to reputation and brand of the company. Oracle Data Masking Pack helps organizations reduce this risk by irreversibly replacing sensitive data with fictitious yet realistic data in non-production environments so that production data can be shared safely in compliance with corporate and government regulations.

KEY FEATURES

- Sensitive Data Discovery and Application Integrity
- Comprehensive and Extensible Mask Format Library
- Secure High Performance Mask Execution
- Sophisticated Masking Techniques
- Automatic self-updates of application mask templates from Oracle

KEY BENEFITS

- Rapid sharing of production data in compliance with data privacy regulations
- Consistent and automatic enforcement of data privacy policies across all enterprise data
- Increased DBA productivity by automating the discovery and masking of sensitive data

RELATED PRODUCTS

Oracle Data Masking Pack delivers maximum benefits when used with the following Oracle Products

- Oracle Test Data Management Pack
- Oracle Real Application Testing
- Oracle Diagnostics Pack
- Oracle Tuning Pack
- Oracle Lifecycle Management Pack

Sensitive Data Identification

Organizations first need to define what sensitive data is in their environment before attempting to mask this information. Oracle Data Masking Pack provides comprehensive data discovery capabilities by allowing security administrators to define data search patterns, such as 15- or 16-digits for credit card numbers, 9-digit formatted US social security numbers or UK national insurance number, to automatically discover sensitive data. The search results are ranked based on how closely they match the search patterns and security administrators can then designate the column as sensitive for inclusion in the data masking process.

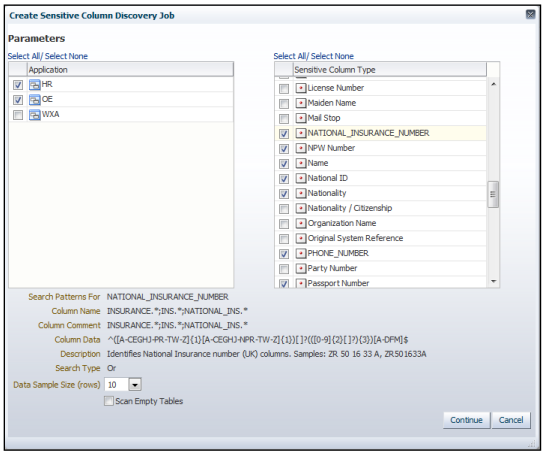


Figure 1. Sensitive data discovery

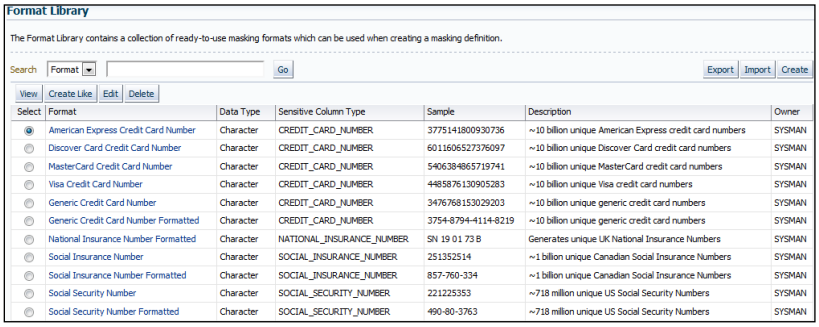
Data Integrity

Defining and identifying sensitive data to mask is first part of the solution. The next and equally challenging task is to preserve referential integrity of the data after masking. Oracle Data Masking Pack automatically detects data dependencies such as foreign key constraints and ensures that referential integrity is maintained during masking. For example, if a sensitive column such as employee number is a primary key in a table relationship, then all associated tables containing dependent columns will be automatically included in the masking process so that the masked value will be consistent across the related tables thus enforcing referential

integrity.

Centralized Masking Rules

Sensitive information can come in a variety of formats. To facilitate their masking, Oracle Data Masking Pack provides a centralized library of mask formats for common types of sensitive data, such as credit card numbers, phone numbers, national identifiers (social security number for US, national insurance number for UK), etc. By leveraging the Format Library in Oracle Data Masking Pack, enterprises can apply data privacy rules to sensitive data throughout the enterprise from a single source and thus, ensure consistent compliance with regulations. Enterprises can also extend this library with their own mask formats to meet their specific data privacy and application requirements.



Select	Format	Data Type	Sensitive Column Type	Sample	Description	Owner
◉	American Express Credit Card Number	Character	CREDIT_CARD_NUMBER	3775141800930736	~10 billion unique American Express credit card numbers	SYSMAN
○	Discover Card Credit Card Number	Character	CREDIT_CARD_NUMBER	6011606527376097	~10 billion unique Discover Card credit card numbers	SYSMAN
○	MasterCard Credit Card Number	Character	CREDIT_CARD_NUMBER	5406384865719741	~10 billion unique MasterCard credit card numbers	SYSMAN
○	Visa Credit Card Number	Character	CREDIT_CARD_NUMBER	4485876130905283	~10 billion unique Visa credit card numbers	SYSMAN
○	Generic Credit Card Number	Character	CREDIT_CARD_NUMBER	3476768153029203	~10 billion unique generic credit card numbers	SYSMAN
○	Generic Credit Card Number Formatted	Character	CREDIT_CARD_NUMBER	3754-8794-4114-8219	~10 billion unique generic credit card numbers	SYSMAN
○	National Insurance Number Formatted	Character	NATIONAL_INSURANCE_NUMBER	SN 19 01 73 B	Generates unique UK National Insurance Numbers	SYSMAN
○	Social Insurance Number	Character	SOCIAL_INSURANCE_NUMBER	251352514	~1 billion unique Canadian Social Insurance Numbers	SYSMAN
○	Social Insurance Number Formatted	Character	SOCIAL_INSURANCE_NUMBER	857-760-334	~1 billion unique Canadian Social Insurance Numbers	SYSMAN
○	Social Security Number	Character	SOCIAL_SECURITY_NUMBER	221225353	~718 million unique US Social Security Numbers	SYSMAN
○	Social Security Number Formatted	Character	SOCIAL_SECURITY_NUMBER	490-80-3763	~718 million unique US Social Security Numbers	SYSMAN

Figure 2. Mask Format Library

Additionally, some sensitive information has complex masking requirements to ensure application data integrity. Oracle Data Masking Pack supports a variety of sophisticated masking techniques such as condition-based masking, compound masking, deterministic masking and key-based reversible masking, to name a few. These out-of-the-box masking techniques allow enterprises to quickly simplify and automate their complex masking requirements while honoring application integrity.

Application Data Masking Templates

Given the complexity of packaged applications, Oracle Data Masking Pack delivers pre-built data masking templates. These templates contain pre-indentified sensitive columns, their relationships and industry standard best practice masking techniques that allow enterprises to obfuscate their packaged applications with confidence while leaving a functional but secure copy for non-production use. The templates are available today for Oracle E-Business Suite and Oracle Fusion Applications.

Inline Masking

With the latest release of Oracle Data Masking Pack, security conscious customers can now take advantage of a new feature, Inline Masking, to obfuscate production data without requiring a staging environment. Masking at the source allows production data to be masked as it is being written out to export files which can then be imported directly into non-production environments without requiring a staging server. Hence sensitive production data never leaves production environments in unmasked form, thus providing the highest level of data security possible.

Secure, High Performance, Efficient, Integrated Mask Execution

Unlike traditional masking processes that are typically slow, Oracle Data Masking Pack uses highly efficient parallelized bulk operations to mask data. It also provides the ability to clone-and-mask via a single workflow. The secure high performance data masking combined with the end-to-end database cloning workflow ensures that enterprises can provision test systems rapidly in hours instead of days or weeks.

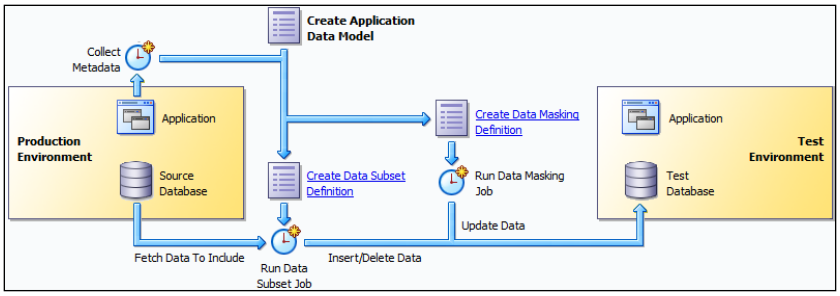


Figure 3. Integrated test data management solution

Data Masking with Test Data Management

Oracle Data Masking Pack is integrated with Test Data Management Pack to allow enterprises to provision a secure system with subset of original data in a single workflow. This eliminates the need for a full copy of the production database which could incur significant storage costs and also ensures that sensitive data never leaves the production system unmasked.

Data Masking and Real Application Testing

The integration of Real Application Testing and Oracle Database Masking enables secure database testing. Oracle Data Masking Pack masks Real Application Testing artifacts like SQL Tuning Sets and workload capture files so that proper testing can be done on test systems where data has been masked. This ensures accurate replay of production workloads while protecting sensitive data from non-production users.

Heterogeneous Data Masking using Oracle Database Gateways

Oracle Data Masking Pack supports masking of data in heterogeneous databases, such as IBM DB2,Microsoft SQL Server, Sybase, Informix, through the use of Oracle Database Gateways

Contact Us

For more information about Oracle Data Masking Pack, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together